CLAIMS

1. A tamper-resistant identity module adapted for physical engagement with a client system having means for receiving digital content over a network and a digital-content usage device, wherein said tamper-resistant identity module comprises a digital rights management (DRM) agent for enabling usage of said digital content.

2. The tamper-resistant identity module according to claim 1, wherein said DRM agent is implemented as an application in an application environment of said tamper-resistant identity module.

3. The tamper-resistant identity module according to claim 2, wherein said DRM agent application is loaded into said identity module application environment from an external trusted party associated with said identity module.

4. The tamper-resistant identity module according to claim 3, wherein said identity module comprises means for authenticating said DRM agent.

5. The tamper-resistant identity module according to claim 1, further comprising means for performing at least part of an authentication and key agreement (AKA) procedure, and said DRM agent includes means for performing DRM processing based on information from said AKA procedure.

6. The tamper-resistant identity module according to claim 5, wherein said DRM agent includes means for extracting a content-protection key to be used for decrypting encrypted digital content provided from a content provider, based on information from said AKA procedure.

7. The tamper-resistant identity module according to claim 1, wherein said DRM agent comprises means for enabling charging for digital content usage.

8. The tamper-resistant identity module according to claim 1, wherein said DRM agent comprises means for managing information related to usage of said digital content, said usage information serving as a basis for charging for digital-content usage.

9. The tamper-resistant identity module according to claim 8, wherein said DRM agent further comprises:

- means for integrity protecting said usage information based on an identity-module specific key; and
- means for sending said integrity protected usage information to an external party managing charging of digital-content usage.

10. The tamper-resistant identity module according to claim 1, wherein said DRM agent implemented in said identity module further comprises means for enabling registration of at least one digital-content usage device.

11. The tamper-resistant identity module according to claim 1, further comprising means for communication between said DRM agent and further DRM functionality implemented in said digital-content usage device based on usage-device specific key information.

12. The tamper-resistant identity module according to claim 11, wherein said communication means is operable for ensuring that only a usage device with valid DRM functionality is enabled to use said digital content.

13. The tamper-resistant identity module according to claim 1, wherein said DRM agent comprises means for receiving, from an external trusted party, a DRM application adapted for use with a digital-content usage device, and means for transferring said DRM application into a tamper-resistant application environment in said digital-content usage device based on usage-device specific key information.

14. The tamper-resistant identity module according to claim 1, wherein said DRM agent implemented in said identity module includes means for checking that the forward-lock function of the Wireless Application Protocol (WAP) is not violated.

15. A client system comprising:

- means for receiving digital content over a network;
- a digital-content usage device;
- a tamper-resistant identity module implemented with a digital rights management (DRM) agent for enabling usage of said digital content by said digital-content usage device.

16. The client system according to claim 15, wherein said DRM agent is implemented as an application in an application environment of said tamper-resistant identity module.

17. The client system according to claim 16, wherein said DRM agent application is loaded into said identity module application environment from an external trusted party associated with said identity module.

18. The client system according to claim 17, wherein said identity module comprises means for authenticating said DRM agent.

19. The client system according to claim 15, wherein said identity module further comprises means for performing at least part of an authentication and key agreement (AKA) procedure, and said DRM agent includes means for performing DRM processing based on information from said AKA procedure.

20. The client system according to claim 19, wherein said DRM agent includes means for extracting a content-protection key to be used for decrypting encrypted

digital content provided from a content provider, based on information from said AKA procedure.

21. The client system according to claim 19, wherein said DRM agent comprises means for enabling charging for digital content usage.

22. The client system according to claim 15, further comprising means for communication between said DRM agent and a further DRM agent implemented in said digital-content usage device based on usage-device specific key information.

23. The client system according to claim 22, wherein said communication means is operable for ensuring that only a usage device with valid DRM functionality is enabled to use said digital content.

24. The client system according to claim 23, wherein said client system further comprises means for transmitting, to a trusted certification party, identification information associated with said digital-content usage device, and in response thereto receiving a protected representation of said usage-device specific key, and said DRM agent comprises means for extracting said usage-device specific key representation for storage in said tamper-resistant identity module.

25. The client system according to claim 15, wherein said digital-content usage device includes a tamper-resistant application environment, and a DRM application adapted for use as a DRM agent in said usage device is loaded into said application environment at least partly based on usage-device specific key information.

26. The client system according to claim 25, wherein said digital-content usage device comprises:

- means for generating new device key information associated with a downloaded DRM application at least partly based on said usage-device specific key information; and
- means for replacing usage-device specific key information stored in said usage device with said new device key information.

27. The client system according to claim 26, wherein said DRM agent implemented in said identity module comprises means for replacing usage-device specific key information stored in said identity module with key information corresponding to said new device key information.

28. A digital rights management (DRM) module comprising:
- a first DRM agent implemented in a tamper-resistant identity module for engagement with a client device, said first DRM agent comprising means for performing first DRM processing associated with digital content;
- a second DRM agent implemented in a digital-content usage device adapted for using said digital content, said second DRM agent comprising means for performing second DRM processing associated with said digital content; and
- means for communication between said first DRM agent and said second DRM agent based on usage-device specific key information.

29. The DRM module according to claim 28, wherein said communication means is operable for ensuring that only a usage device with valid DRM functionality is enabled to use said digital content.

30. The DRM module according to claim 28, wherein said tamper-resistant identity module comprises means for performing at least part of an authentication and key agreement (AKA) procedure, and said means for performing first DRM processing in said first DRM agent operates based on information from said AKA procedure.

31. The DRM module according to claim 30, wherein said means for performing first DRM processing in said first DRM agent includes means for extracting a content-protection key to be used for decrypting protected digital content from a content provider, based on information from said AKA procedure.

32. The DRM module according to claim 31, wherein said communication means is operable for ensuring that said content-protection key is accessible only by a second DRM agent that properly enforces usage rules associated with said digital content.

33. The DRM module according to claim 32, wherein said means for performing second DRM processing in said second DRM agent comprises means for decrypting encrypted digital content by means of said content-protection key.

34. The DRM module according to claim 30, wherein said means for performing first DRM processing in said first DRM agent comprises means for enabling charging for said digital content.

35. The DRM module according to claim 28, wherein said first DRM agent comprises:

- means for authenticating said usage device based on said usage-device specific key information to verify that said usage device has valid DRM functionality; and
- means for sending DRM data enabling usage of said digital content to said second DRM agent in response to successful authentication of a usage device with valid DRM functionality.

36. The DRM module according to claim 28, wherein said first DRM agent comprises:

- means for encrypting DRM data enabling usage of said digital content, based on said usage-device specific key information; and

- means, forming part of said communication means, for sending said encrypted DRM data to said second DRM agent; and

said second DRM agent comprises means for decrypting said encrypted DRM data to enable usage of said digital content, based on said usage-device specific key information.

37. The DRM module according to claim 28, wherein said tamper-resistant identity module and said usage device are tamper-resistantly configured with usage-device specific key information.

38. The DRM module according to claim 28, wherein said second DRM agent comprises means for compiling information related to usage of said digital content, and means for transferring said usage information to said first DRM agent based on said usage-device specific key information; and

said first DRM agent comprises means for sending said usage information to an external party managing charging of digital-content usage, said usage information serving as a basis for charging for digital-content usage.

39. The DRM module according to claim 28, wherein said second DRM agent comprises means for sending a first control signal related to the digital-content usage process to said first DRM agent, and said first DRM agent comprises means for processing signal data associated with said first control signal to generate a second control signal, and means for sending said second control signal to said second DRM agent for controlling said digital-content usage process.

40. The DRM module according to claim 28, wherein said first DRM agent is implemented as an application in an application environment of said tamper-resistant identity module.

41. The DRM module according to claim 40, wherein said first DRM agent application is loaded into said identity module application environment from an external trusted party associated with said identity module.

42. The DRM module according to claim 40, wherein said identity module comprises means for authenticating said DRM agent.

43. The DRM module according to claim 28, wherein said second DRM agent is implemented as an application in a tamper-resistant application environment in said usage device.

44. The DRM module according to claim 43, wherein said second DRM agent application is loaded into said usage-device application environment at least partly based on said usage-device specific key information.

45. The DRM module according to claim 44, wherein said digital-content usage device comprises:

- means for generating new device key information associated with said downloaded DRM application at least partly based on said usage-device specific key information; and
- means for replacing usage-device specific key information stored in said usage device with said new device key information.

46. The DRM module according to claim 45, wherein said DRM agent implemented in said identity module comprises means for replacing usage-device specific key information stored in said identity module with key information corresponding to said new device key information.

47. A method for digital rights management (DRM) comprising the steps of:

- tamper-resistantly configuring a usage device, adapted for using digital content, with a usage-device specific key;
- providing a cryptographic representation of said usage-device specific key to a client device associated with said usage device;
- processing, at a trusted certification party, said cryptographic representation received in a request from said client device to retrieve key information representative of said usage-device specific key;
- securely transferring said key information from said trusted certification party to a tamper-resistant identity module in said client device, based on an identity-module specific key; and
- establishing communication between a first DRM agent in said tamper-resistant identity module and a second DRM agent in said usage device based on the key information transferred to the identity module and the usage-device specific key in said usage device.
